Supreme Court, U.S.
FILED
DEC 3 - 2003
OFFICE OF THE CLERK

No. 03-658

IN THE

Supreme Court of the United States

JOHN DEEP,

Petitioner,

v.

THE RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC., *ET AL.*,

Respondents.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Seventh Circuit

BRIEF OF *AMICUS CURIAE* CHARLES LEE MUDD JR., PRESIDENT AND ATTORNEY, PRIVACY INNOVATIONS INC. IN SUPPORT OF PETITIONER

Charles Lee Mudd Jr.
4710 North Virginia Avenue
Chicago, Illinois 60625
773.271.7600
Counsel for Amicus

Date: December 2, 2003

TABLE OF CONTENTS

Pages

TABLE OF CONTENTS 2
TABLE OF AUTHORITIES ii
INTEREST OF AMICUS CURIAE 1
ARGUMENT 2
I. The Rules Advocated By the Court Below Would Undermine This Court's *Betamax* Decision and Thereby Cause Irreparable Harm to the Information Technology and Internet Industries. ... 2
II. Review Is Necessary to Ensure that Lower Courts Will Not Exceed Their Authority by Penalizing Compliance with the ECPA and Other Privacy Related Statutes and Regulations. 7
CONCLUSION 13

TABLE OF AUTHORITIES

Pages

Cases

A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001) 1, 3

In re: Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003) 3, 4, 8, 10, 11

Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984) 1, 2, 3, 7

Statutory and Legislative Authorities

17 U.S.C. § 512(i)(2)(A) 6

17 U.S.C. § 1201(c)(3) 5-6

18 U.S.C. §§ 2510, 2511 8

16 C.F.R. 313 9

45 C.F.R. §§160, 164 9

65 Fed. Reg. 101, 33646 9

Other Authorities

Apple Corporation, Press Release, iTune Music Store Hits Five Million Downloads (June 23, 2003) 12

Benny Evangelista, *Download Lawsuit Dismissed; RIAA Drops Claim That Grandmother Stole Online Music*, San Francisco Chronicle, September 25, 2003, at B1 11

Brett Sporich, *DVD Boom Continues*, Billboard, August 16, 2003, at 42. 3

C.J. Alice Chen and Aaron Burstein, *The Law and Technology of Digital Rights Management*, 18 Berkeley Tech. L.J. 487, 491 (2003) 7

Edward W. Felten, *A Skeptical View of DRM and Fair Use*, Communications of the ACM (April 2003) at 57, 58 7

European Union Data Directive 95/46/EC, Article 17 9

Frank Ahrens, *RIAA's Lawsuits Meets Surprised Targets: Single Mother in Calif., 12 Year-Old Girl in N.Y. Among Defendants*, Washington Post, September 10, 2003, at E1 11

Masanobu Katoh, *Intellectual Property and the Internet: A Japanese Perspective*, 2002 U. Ill. J. L. Tech. & Policy 333, 342-347 (2002) 5

Ninth Circuit Appeal Nos. 03-55894 and 03-55901 from Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F. Supp.2d 1029, (C.D. Cal. 2003), MGM Plaintiff-Appellants' Opening Brief at 42 ("MGM Brief"); Brief in Support of Reversal by *Amici Curiae* Law Professors and Treatise Authors at 22-23 ("Boorstyn Brief"); Brief of *Amici Curiae* of FullAudio Corp. *et al.* at 17-18 ("FullAudio Brief"); Brief of *Amici Curiae* American Film Marketing Association *et al.* at 14 ("AFMA Brief") 3

S. 2048, the Consumer Broadband and Digital Television Promotion Act 5

Tim Knauss, *Lawsuits Scare Off CNY Music Downloaders*, Syracuse Post Standard, September 14, 2003, at A1 11

INTEREST OF AMICUS CURIAE[1]

This Court in *Sony Corp. of America v. Universal City Studios*, 464 U.S. 417 (1984) ("*Betamax*"), and the Ninth Circuit in *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001)("*Napster*"), created fair and practical rules for secondary copyright liability. These rules have unleashed the creative powers of the information technology industry and led directly to the growth of the Internet. The court below now seeks to change these rules, and replace them with new standards that would as a practical matter give the entertainment industry a veto power over the development of innovative products and services. This change in the rules would wreck havoc in the information and technology industries, and would harm users of digital information.

Amicus does not condone the infringement that occurs over the Internet in general and peer-to peer networks in particular. However, the misinterpretation of *Betamax* is not the proper solution to this problem. Accordingly, this Court should reject the misreading of *Betamax* urged by the court below.

ARGUMENT

I. The Rules Advocated By the Court Below Would Undermine This Court's *Betamax* Decision and Thereby Cause Irreparable Harm to the Information Technology and Internet Industries.

This case is about more than the legality of peer-to-peer software. It is about the future of the information technology ("IT") industry, the Internet, and the fair use of digital works.

---

[1] No counsel for a party authored this brief in whole or in part, nor did any person or entity other than *amicus* or its counsel make a monetary contribution to the preparation or submission of this brief. This brief is filed with the written consent of all parties.

The legal foundation upon which the IT industry stands is this Court's decision in *Betamax*. In *Betamax*, this Court proclaimed that the manufacturer of a product could not be held secondarily liable for infringing uses of the product so long as the product was capable of substantial noninfringing uses. That clear standard gave venture capitalists, engineers, and manufacturers the confidence and certainty that they could invest their resources in developing a wide range of consumer IT products without facing copyright liability. These products include personal computers, laptops, scanners, printers, and the software that enables them to operate.

Prior to the sale of these products, the investors and manufacturers have known that consumers could use them to infringe the copyrights in computer programs, computer games, sound recordings, motion pictures, and many literary works. And once the products have been on the market, the investors and manufacturers have known for a certainty that some consumers have in fact used the products for infringing purposes. The investors and manufacturers likewise have known that government and business employees have used their workplace computers to make infringing copies, although perhaps to a lesser degree than their home computers. Nonetheless, under the *Betamax* standard, the investors and manufacturers have also known that they were safe from copyright liability because these products were all capable of substantial noninfringing uses.

In the nearly twenty years since the *Betamax* decision, the IT revolution has created millions of jobs in the U.S. and abroad. It has increased the productivity of businesses, and dramatically enhanced people's ability to access and use information. Although digital technology has exposed the entertainment industry to copyright infringement, it has also benefited the entertainment industry in numerous ways. Computer graphics are routinely used in the production of both live action and animated films and television shows to

make special effects look more realistic. Digital recording technology enables a small number of musicians and technicians to create the sound of an orchestra. Digital storage media such as compact discs and digital versatile discs ("DVDs") provide consumers with previously unimaginable audio and video quality. DVDs have created a huge new market for the picture industry -- $ 11.7 billion in 2002 alone.[2]

The court below contends that the Ninth Circuit, in *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001)("*Napster*"), misapplied this Court's *Betamax* decision. But the court below also advocates significantly limiting the applicability of *Betamax*, and replacing this Court's holdings in *Betamax* with its own. Indeed, Respondents and their *amici* have already begun to rely extensively on the holdings of the court below – while replacing the holdings of *Betamax* – in briefs filed in closely related Ninth Circuit Appeals from *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp.2d 1029, (C.D. Cal. 2003).[3]

In *Aimster*, Judge Posner explicitly disagreed with the Ninth Circuit in *Napster* and implicitly disagreed with *Betamax*. *Aimster*, 334 F.3d at 649. Judge Posner read into *Betamax* a non-existent cost-benefit test, stating that "when a supplier is offering a product or service that has noninfringing as well as infringing

---

[2] Brett Sporich, *DVD Boom Continues*, Billboard, August 16, 2003, at 42.

[3] *See, e.g.*, Appeal Nos. 03-55894 and 03-55901, MGM Plaintiff-Appellants' Opening Brief at 42 ("MGM Brief"); Brief in Support of Reversal by *Amici Curiae* Law Professors and Treatise Authors at 22-23 ("Boorstyn Brief"); Brief of *Amici Curiae* of FullAudio Corp. *et al.* at 17-18 ("FullAudio Brief"); Brief of *Amici Curiae* American Film Marketing Association *et al.* at 14 ("AFMA Brief"), available at http://www.eff.org/IP/P2P/MGM_v_Grokster/

uses, some estimate of the respective magnitudes of these uses is necessary for a finding of contributory infringement." *Id.* Later, Judge Posner articulated the following rule: "Even when there are noninfringing uses of an Internet file-sharing service ... if the infringing uses are substantial then to avoid liability as a contributory infringer the provider of the service must show that it would have been disproportionately costly for him to eliminate or at least reduce substantially the infringing uses." *Id.* at 653.

This rule, if adopted nationwide, could cripple the IT industry. In order to avoid copyright liability, a company that marketed a product would have to constantly assess: 1) whether the infringing uses were substantial; and 2) if they were substantial, whether the infringements could be reduced or eliminated in a manner that would not be disproportionately costly. Judge Posner did not define how substantial the infringing uses would have to be, nor how disproportionate the costs of avoiding the infringement. Judge Posner also did not appreciate how costly and technically difficult it can be for a provider of technology products or services to monitor their use and determine whether the use infringed copyright. Since virtually all IT products have some infringing uses, manufacturers and service providers would operate in a perpetual state of uncertainty and confront unending litigation as copyright owners and courts second guessed every engineering decision the manufacturers made.

But if P2P software distributors have a legal duty to use infringement filters, so too do all other software and hardware firms. This rule would require Microsoft to redesign Windows to filter out infringing works and prevent the transmission of infringing material over the Internet. Hewlett-Packard would be forced to reengineer its personal computers to preclude the installation of P2P software. AOL would be required to reconfigure its email and instant messaging service to

inhibit the attachment of files containing infringing works.

In other words, the court below recasts secondary liability as a means of requiring IT companies to implement digital rights management ("DRM") systems. But the court below should not grant what Congress has already denied.

In March 2002, Senator Ernest Hollings of South Carolina, Chairman of the Senate Commerce Committee, introduced S. 2048, the Consumer Broadband and Digital Television Promotion Act. The Hollings bill would have given copyright owners, consumer groups, and the manufacturers of digital media devices twelve months to reach an agreement on "security system standards for use in digital media devices...."[4] If within those twelve months the parties reached an agreement, the Federal Communications Commission ("FCC") would have adopted those standards as a legally binding regulation. On the other hand, if the parties did not reach agreement, the FCC would have been required to initiate a rulemaking proceeding to adopt a standard.

The Hollings bill came under sharp attack from the IT industry, which questioned the bill's assumptions and substance.[5] Additionally, the bill's requirement that IT companies include DRM systems represented a departure from the legislative compromise of Title I of the Digital Millennium Copyright Act ("DMCA"). The IT industry had agreed to the DMCA's prohibition on the

---

[4] Digital media devices were defined broadly enough to include all computers and consumer electronic devices such as CD and DVD players.

[5] For a more detailed discussion of the Hollings bill, see Masanobu Katoh, *Intellectual Property and the Internet: A Japanese Perspective*, 2002 U. Ill. J. L. Tech. & Policy 333, 342-347 (2002).

manufacture of circumvention devices and components only because of the inclusion of the "no mandate clause" in 17 U.S.C. § 1201(c)(3): "Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure...." Notwithstanding this provision, the Hollings bill would have required all digital media devices to respond to the security system standards established pursuant to the legislation.

The Hollings bill also departed from the legislative compromise in Title III of the DMCA. One of the conditions for an Internet service provider to be eligible for the DMCA's safe harbors was that it accommodated and did not interfere with standard technical copyright protection measures that had been developed "pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary multiindustry standards process." 17 U.S.C. § 512(i)(2)(A). A security system developed and mandated by the FCC obviously differs from a consensus standard developed pursuant to a voluntary multi-industry process.

Because of the strong opposition it aroused, the Hollings bill did not progress beyond the Senate Commerce Committee, and it died with the end of the 107th Congress. Congress having refused to reverse its "no mandate" policy judgment in the DMCA, the court below reached essentially the same result by means of expansive application of the secondary liability doctrine.

Should the decision of the court below stand, the entertainment industry will be empowered to dictate to the IT industry how to design its products. To avoid endless cycles of copyright litigation, IT companies will have no choice but to include whatever DRM systems the entertainment industry demands. These DRM sys-

tems could inhibit the functionality of IT products and impede innovation. Additionally, the DRM systems inevitably will diminish users' ability to make lawful copies. This is because it is impossible to design a DRM system that can distinguish between fair uses and infringing uses.[6] Thus, a DRM system that effectively prevents infringing uses will also prevent some fair uses.

In short, the contributory infringement and vicarious liability standards advocated by the court below would fundamentally change the character of the IT industry in this country. Instead of a highly innovative and competitive sector, where new products are rushed to market in an effort to satisfy consumer demand and capture market-share, the IT industry will be regulated by copyright lawyers from the entertainment industry. These lawyers will second guess every engineering decision made by every IT company, and will insist upon DRM systems that limit the many lawful uses recognized by Congress and the courts. This result is precisely what this Court rejected in *Betamax*: enlargement of "the scope of respondents' statutory monopolies to encompass control over an article of commerce that is not subject to copyright protection." *Betamax*, 464 U.S. at 421.

II. Review Is Necessary to Ensure that Lower Courts Will Not Exceed Their Authority by Penalizing Compliance with the ECPA and Other Privacy Related Statutes and Regulations

The opinion from the court below also imposes an unforeseen and unexpected burden upon developers of

---

[6] Edward W. Felten, *A Skeptical View of DRM and Fair Use*, Communications of the ACM (April 2003) at 57, 58; C.J. Alice Chen and Aaron Burstein, *The Law and Technology of Digital Rights Management*, 18 Berkeley Tech. L.J. 487, 491 (2003).

technology and providers of communication services. This burden imposed by the court below involves the balance between advancing privacy enhancing technologies and avoiding the penalties such efforts can now impose. For, the court below has indeed penalized Petitioner for the use of encryption technology. Indeed, the court below chastises and, in fact, penalizes Petitioner for the employment of encryption technology. See *Aimster*, 334 F.3d at 650 (". . . no more can Deep by using encryption software to prevent himself from learning what surely he strongly suspects to be the case: that the users of his service - maybe all the users of his service - are copyright infringers"). While the court below thereafter cushions its edict, the theme remains clear that the court below viewed the use of encryption technology as a means to avoid learning the nature of the communications in which Aimster's users engaged. By doing so, the court below has imposed a burden inconsistent with federal law that elsewhere imposes the obligation to protect the security of communications and refrain from unauthorized interception of electronic communications.

Under the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510, et seq., any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . shall be punished . . . or shall be subject to suit." 18 U.S.C. § 2511. The same penalties would also apply to anyone who disclosed any information knowing that the information may have been obtained through the interception of a covered communication. *See id.* Consequently, Petitioner is precluded under the ECPA from intercepting the electronic communications of those individuals to whom it provides communications services absent some other legal authority. *See id.* Thus, the implied burden imposed upon Petitioner by the court below to learn or be aware of the communications of its subscribers would quite likely violate the

ECPA. *See id.* From the perspective of the ECPA, the use of encryption technology to preclude the interception of the communications by Petitioner and other third parties reflects valiant efforts to comply with the statute's intent. Indeed, such use of encryption seems logical.

In addition to the ECPA, other statutes and regulations promulgated by federal and state legislative bodies impose a burden on certain entities to implement measures to ensure the security of information obtained by and from consumers and customers. While Petitioner likely does not fall within the scope of the Health Information Portability and Accountability Act ("HIPAA"), the use of encryption along with the file-sharing technology could permit physicians and other health care practitioners to utilize the Aimster services to share patient medical information and related files knowing a level of security compliant with HIPAA exists. *See* Standard for Privacy of Individually Identifiable Health Information and Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. §§160, 164 (2000-2003). This would also apply to those individuals and entities falling within the scope of the Financial Modernization Act ("Gramm-Leach-Bliley"). *See* Privacy of Consumer Financial Information; Final Rule, 16 C.F.R. 313 (2000); 65 Fed. Reg. 101, 33646 (2000). Without encryption and security enhancing technology, these uses would likely be precluded by privacy and security concerns. Looking to a broader perspective as articulated in the European Union Data Directive 95/46/EC, Petitioner's use of security technology complies with Article 17 of the Directive which requires the implementation of "appropriate technical and organizational measures to protect personal data against . . . unauthorized alteration, disclosure or access, in particular where the processing involves the transmission of data over a network . . . ." Eur. Parl. Direct. 95/46/EC (1995). Again, in this light, the Petitioner's use of encryption seems logical.

The court below counteracts the efforts of privacy initiatives that promote the use of technology that provides for the secure and confidential transmission of electronic communications. By suggesting throughout a substantial portion of the opinion that Petitioner has somehow diminished the viability of its claims by employing the use of encryption technology (most pronounced when described as having caused a "self-inflicted wound"), the court below sends a message to the IT community and developers of communications services that the employment of security technology (eg. encryption) to secure electronic communications diminishes the viability of a defense to potential copyright infringement claims based on alleged conduct of their users and/or subscribers. Indeed, the court below advocates an approach that could easily be interpreted as quite inconsistent with the ECPA and privacy efforts of the last two decades. The court below implicitly advocates the interception and monitoring of electronic communications by Internet Service Providers (perhaps except those that would fall within the protections afforded by the surviving portions of the Communications Decency Act and the Digital Millenium Copyright Act) to avoid potential liability. Moreover, the court below warns that the use of technology to preclude such interception and monitoring of electronic communications may very well be construed against one in defending claims of contributory infringement. Consequently, the opinion of the court below creates a chilling effect on the advancement of privacy enhancing technologies. Such an approach seems illogical.

The court below asserts that Petitioner may have specifically structured his technology so that he could avoid secondary liability for the infringing activities of users of his software, characterizing such a deliberate attempt, if proven, as "willful blindness." *Aimster* at 650-651. *Amici* take no position on this factual dispute. However, *amici* note that there has been no trial and that Petitioner has presented apparently undis-

puted evidence at least of the noninfringing use of his Aimster Internet service for the sale of licensed music, Petition at 5-6.

Nonetheless, the court below correctly recognized that this Court made clear in *Sony* that the manufacturer of a product could not be held secondarily liable for infringing uses of the product so long as the product was capable of substantial noninfringing uses. *In re Aimster*, 334 F.3d at 649 ("The [Supreme] Court was unwilling to allow copyright holders to prevent infringement effectuated by means of a new technology at the price of possibly denying noninfringing consumers the benefit of the technology.").

We understand Respondents frustration with P2P networks and with the *Betamax* and *Napster* decisions. But the secondary liability rules advocated by the court below would cause irreparable injury to the IT industry, Internet companies, and users. In the long run, these rules will also harm Respondents, who will be denied markets that the IT industry otherwise would have created for them.

But Respondents are not powerless to combat infringement over P2P networks. Two recent developments prove the opposite. First, the Recording Industry Association of America (RIAA) has begun to sue individual file traders engaged in large scale infringement. While the RIAA may not have selected all its targets wisely,[7] this strategy appears to have caused a de-

---

[7] *E.g.*, Frank Ahrens, *RIAA's Lawsuits Meets Surprised Targets: Single Mother in Calif., 12 Year-Old Girl in N.Y. Among Defendants*, Washington Post, September 10, 2003, at E1; Benny Evangelista, *Download Lawsuit Dismissed; RIAA Drops Claim That Grandmother Stole Online Music*, San Francisco Chronicle, September 25, 2003, at B1.

crease in file trading.[8]

Second, legal downloads of sound recordings are finally available in a low cost, user-friendly manner. In iTunes' first two months of operation, for example, users downloaded over five million songs for 99 cents a piece.[9] The combination of vigorous enforcement against hard core infringers and attractive business models for legal downloads should solve appellants' problems with P2P networks without crippling the IT industry.

Finally, the court below has improperly burdened the Petitioner by penalizing its use of privacy enhancing technology and reluctance to monitor its users' and subscribers' communications. This burden could significantly affect the development and use of privacy enhancing technologies by the IT industry. In turn, the reluctance to develop and use privacy enhancing technologies will affect consumers negatively. Moreover, the court below has arguably placed its decision before compliance with the ECPA and other privacy related statutes and regulations. Therefore, this Court should reject the approach adopted by the court below."

---

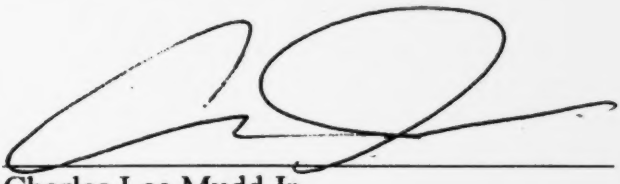
[8] Tim Knauss, *Lawsuits Scare Off CNY Music Downloaders*, Syracuse Post Standard, September 14, 2003, at A1.

[9] Press Release, Apple Corporation, iTune Music Store Hits Five Million Downloads (June 23, 2003).

CONCLUSION

For the foregoing reasons, the Petition for Writ of Certiorari should be granted.

Respectfully submitted,



Charles Lee Mudd Jr.
Counsel
Member, United States Supreme Court Bar
Admitted 25 June 2001